PARTIAL TRANSLATION OF JP 10(1998)-162088 A

Publication Date: June 19, 1998
Title of the Invention: ELECTRONIC MONEY SYSTEM, AND ILLEGAL CARD DETECTION METHOD
Patent Application Number: 8-321251
Filing Date: December 2, 1996
Inventors: Toshihide IIDA et al.
Applicant: NTT DATA TSUSHIN KK

(Page 5, left column, lines 19 – 36)
[0013] In an electronic money system according to the above-mentioned first and second viewpoints, it may be possible that physical features of a bearer of the electronic money card is stored in the electronic money card, physical features of a user of the electronic money card are read and matched with those stored in the electronic money card to determine whether or not a similarity is equal to or higher than a predetermined value, and in the case where the similarity is equal to or higher than the predetermined value, transmission of the transaction request is permitted.

[0014] According to the above-mentioned configuration, when an electronic money card is used, physical features of a user are read and matched with those of a card bearer stored in the electronic money card, whereby it is determined whether or not the user is the bearer of the electronic money card. Because of this, a third party can be prevented from pretending to be a bearer of an electronic money card and using the electronic money card.

[0015] The physical features include either information on a fingerprint, a voice print, a face picture, and a retina pattern, for example.

(Page 10, right column, lines 7 – 21)
[0071] Furthermore, individual particular information representing

individual physical features such as a voice print, a face pattern, and a retina pattern may be used in place of fingerprint data, or may be combined with fingerprint data. For example, the following may possible: a microphone is disposed as an individual information reading part 34; feature data of a voice obtained through the microphone is extracted; relative intensity of the feature data thus obtained with respect to that of a voice stored in an IC part 20 is determined; and in the case where the relative intensity is equal to or higher than a predetermined value, an operator is authenticated, whereby the use of a system is permitted.

[0072] Furthermore, in the case of using a face pattern, a retina pattern, and the like, it may be possible that feature data of a face pattern and a retina pattern is stored in the IC part 20, feature data of a picture captured by a camera is extracted, relative intensity of the feature data thus extracted with respect to that stored in the IC part 20 is determined, and in the case where the relative intensity is equal to or higher than a predetermined value, an operator is authenticated.

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10162088 A**

(43) Date of publication of application: **19.06.98**

(51) Int. Cl **G06F 19/00**
G07D 9/00
G07D 9/00
G07D 9/00
G07F 7/08

(21) Application number: **08321251**

(22) Date of filing: **02.12.96**

(71) Applicant: **N T T DATA TSUSHIN KK**

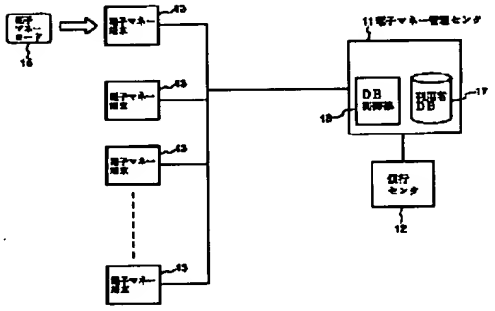
(72) Inventor: **IIDA TOSHIHIDE**
TAKAGI TAKASHI

(54) **ELECTRONIC MONEY SYSTEM, AND ILLEGAL CARD DETECTION METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an electronic money system that can effectively prevent the illegal use of a forged electronic money card.

SOLUTION: An electronic money terminal 13 transmits a transaction request containing an identification code stored in the electronic money card 15 and a check code to an electronic money management center 11. The electronic money management center 11 discriminates whether the check code of the electronic money card 15 contained in the received transaction request is matched with the check code of the electronic money card 15 on user DB(data base) 17 storing the check codes of the respective electronic money cards 15. When they are not matched, transaction is stopped. The electronic money management center 11 gives an instruction to the electronic money terminal 13 so that it updates the check code on user DB17 and updates the check code on the electronic money card 15 to the same value after transaction completes. The electronic money terminal 13 updates the check code on the electronic money card 15 in accordance with the instruction.



(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平１０－１６２０８８

(43)公開日　平成10年(1998)6月19日

(51)Int. Cl.[6]		識別記号	F I		
Ｇ０６Ｆ	19/00		Ｇ０６Ｆ	15/30	３５０　Ａ
Ｇ０７Ｄ	9/00	４５１	Ｇ０７Ｄ	9/00	４５１　Ｂ
		４５６			４５６　Ｅ
		４６１			４６１　Ｚ
					４６１　Ａ

審査請求　未請求　請求項の数１２　ＯＬ　(全１３頁) 最終頁に続く

(21)出願番号　特願平8-321251

(22)出願日　平成8年(1996)12月2日

(71)出願人　000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目3番3号

(72)発明者　飯田　利英
東京都江東区豊洲三丁目3番3号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　高木　孝
東京都江東区豊洲三丁目3番3号　エヌ・ティ・ティ・データ通信株式会社内

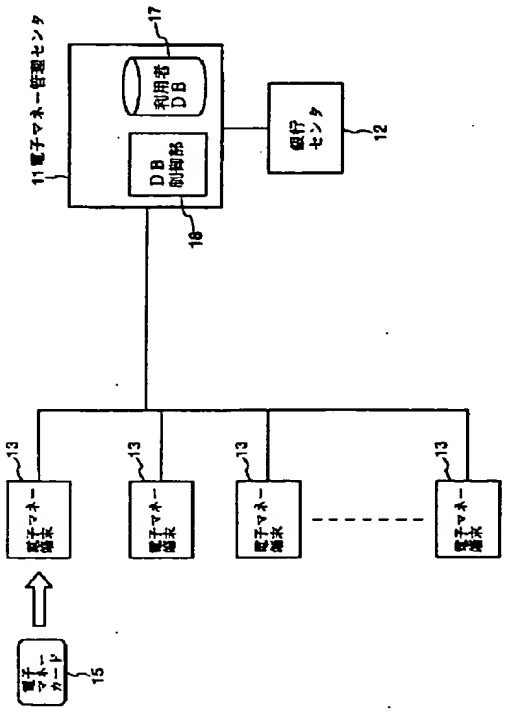
(74)代理人　弁理士　木村　満

(54)【発明の名称】電子マネーシステム及び不正カード検出方法

(57)【要約】

【課題】　電子マネーカードの偽造カードの不正使用を有効に防止することができる電子マネーシステムを提供する。

【解決手段】　電子マネー端末１３は、電子マネーカード１５に記憶された識別符号とチェックコードを含む取引要求を電子マネー管理センタ１１に送信する。電子マネー管理センタ１１は、受信した取引要求に含まれる電子マネーカード１５のチェックコードと、各電子マネーカード１５のチェックコードを記憶する利用者ＤＢ１７上の同電子マネーカード１５のチェックコードが一致するか否かを判別し、一致しない場合取引を中止する。取引完了後、電子マネー管理センタ１１は、利用者ＤＢ１７上のチェックコードを更新すると共に電子マネーカード１５上のチェックコードも同一の値に更新するよう電子マネー端末１３に指示する。電子マネー端末１３は、指示に従って、電子マネーカード１５上のチェックコードを更新する。



1

【特許請求の範囲】

【請求項１】金銭的価値を有する電子マネーを格納する電子マネーカードと、該電子マネーカードを処理するための端末と、該端末を制御するセンタとを備え、前記電子マネーカード間で前記電子マネーを取引する電子マネーシステムであって、

前記電子マネーカードは、該電子マネーカードを特定するための識別符号と、チェックコードとを記憶する手段を備え、

前記端末は、前記電子マネーカードに記憶されている前記チェックコードと前記識別符号とを含む取引要求を前記センタに送信する送信手段を備え、

前記センタは、各前記電子マネーカードの前記チェックコードを記憶するチェックコード記憶手段と、前記チェックコード記憶手段に記憶されている前記チェックコードのうち、前記端末からの前記取引要求に含まれている前記識別符号により特定される前記電子マネーカードの前記チェックコードが前記取引要求に含まれている前記チェックコードと一致するか否かを判別する判別手段と、前記チェックコードが一致すると判別された場合、取引を許可し、前記チェックコードが一致しないと判別された場合、取引を中止する制御手段と、取引が許可された場合、前記電子マネーカードに対して新たにチェックコードを生成する生成手段と、前記チェックコード記憶手段に記憶されている該電子マネーカードの前記チェックコードを前記生成手段により生成された前記チェックコードに更新する第１の更新手段と、前記端末に装着されている前記電子マネーカードに記憶されている前記チェックコードを前記チェックコード記憶手段に記憶されているチェックコードと同一の値に更新するよう指示する手段と、を備え、

前記端末は、前記センタからの指示に応答して、装着されている前記電子マネーカードの前記チェックコードを更新する第２の更新手段を更に備える、

ことを特徴とする電子マネーシステム。

【請求項２】前記制御手段は、前記判別手段により前記チェックコードが一致しないと判別された場合、不正検出を通知する手段を更に備える、

ことを特徴とする請求項１に記載の電子マネーシステム。

【請求項３】前記第１の更新手段は、更新前の前記チェックコードを記憶する使用済チェックコード記憶手段を更に備え、

前記制御手段は、前記判別手段により前記チェックコードが一致しないと判別された場合、前記電子マネーカードに記憶されている前記チェックコードが前記使用済チェックコード記憶手段に記憶されているチェックコードのいずれかと一致するか否かを判別し、一致した場合、不正に複製されたコピーカードの検出を通知する手段を更に備える、

2

ことを特徴とする請求項１、又は２に記載の電子マネーシステム。

【請求項４】前記電子マネーカードは、該電子マネーカードの保有者の身体的特徴を記憶する手段を更に備え、

前記端末は、前記電子マネーカードの利用者の身体的特徴を読み取る特徴読取手段と、該端末に装着された前記電子マネーカードに記憶されている前記身体的特徴を読み出し、前記特徴読取手段により読み取られた身体的特徴と比較し、類似度が一定値以上か否かを判別する手段と、類似度が一定値以上であると判別された場合、前記送信手段に前記取引要求の送信を許可する手段と、を更に備える、

ことを特徴とする請求項１乃至３のいずれか１項に記載の電子マネーシステム。

【請求項５】前記生成手段は、乱数を用いて新たなチェックコードを生成する手段を更に備える、

ことを特徴とする請求項１乃至４のいずれか１項に記載の電子マネーシステム。

【請求項６】前記電子マネーカードは、光エネルギーが照射されることにより物理的にピットが形成されてデータが書き込まれ、書き換えが実質的に不可能な光記憶部を備え、該光記憶部に取引に関する情報を記録する、

ことを特徴とする請求項１乃至５のいずれか１項に記載の電子マネーシステム。

【請求項７】金銭的価値を有する電子マネーを格納する電子マネーカードを用いて前記電子マネーを取引する電子マネーシステムにおいて、

前記電子マネーカードは、前記電子マネーカードを特定するための識別符号とチェックコードを記憶する記憶手段を備え、

前記電子マネーカードに記憶されている前記チェックコードと前記識別符号とを読み出す読出手段と、

各前記電子マネーカードの前記識別符号と前記チェックコードを関連付けて記憶するチェックコード記憶手段と、

前記チェックコード記憶手段に記憶されるチェックコードのうち、前記読出手段により読み出された前記識別符号に対応する前記チェックコードと、前記読出手段により読み出された前記チェックコードが一致するか否かを判別するコード判別手段と、

前記コード判別手段により前記チェックコードが一致すると判別された場合、取引を許可し、前記チェックコードが一致しないと判別された場合、取引を中止する制御手段と、

取引が許可された場合、前記電子マネーカードに対して新たにチェックコードを生成する生成手段と、

前記チェックコード記憶手段に記憶されている前記チェックコードのうち、該電子マネーカードの前記チェックコードを前記生成手段により生成された前記チェックコードに更新する手段と、

前記電子マネーカードに記憶されている前記チェックコードを前記チェックコード記憶手段に新たに記憶されるチェックコードと同一の値に更新する手段と、
を備える、ことを特徴とする電子マネーシステム。
【請求項８】前記電子マネーカードの保有者の身体的特徴を記憶する特徴記憶手段と、
前記電子マネーカードの利用者の身体的特徴を読み取る特徴読取手段と、
前記特徴記憶手段に記憶された前記身体的特徴と前記特徴読取手段により読みとられた身体的特徴を比較し、それらの類似度が一定値以上か否かを判別する類似度判別手段と、
前記類似度判別手段により類似度が一定値以上であると判別された場合、取引を許可する手段と、
を更に備えることを特徴とする請求項７に記載の電子マネーシステム。
【請求項９】前記身体的特徴は、指紋、声紋、顔の画像、網膜パターンに関する情報のいずれかを含む、ことを特徴とする請求項４、又は８に記載の電子マネーシステム。
【請求項１０】金銭的価値を有する電子マネーを格納する電子マネーカードを用いて前記電子マネーを取引する電子マネーシステムにおいて、
前記電子マネーカードはチェックコードを記憶し、
各前記電子マネーカードの前記チェックコードを記憶するチェックコード記憶手段と、
取引に用いる前記電子マネーカードに記憶される前記チェックコードが、前記チェックコード記憶手段に記憶されている前記チェックコードのうちの前記取引に用いる電子マネーカードの前記チェックコードと一致するか否かを判別し、一致する場合取引を許可し、一致しない場合取引を中止すると共に不正検出を通知する判別手段と、
取引が許可された場合、前記電子マネーカードに記憶されている前記チェックコードと前記チェックコード記憶手段に記憶されている前記電子マネーカードの前記チェックコードとを同一の新たな値に更新する手段と、
を備える、ことを特徴とする電子マネーシステム。
【請求項１１】金銭的価値を有する電子マネーを格納する電子マネーカードを用いて前記電子マネーを取引する電子マネーシステムにおいて、
各前記電子マネーカードを特定するための識別符号とチェックコードを該電子マネーカードに記憶させる記憶ステップと、
前記電子マネーカードから前記チェックコードと前記識別符号とを読み出す読出ステップと、
各前記電子マネーカードの前記識別符号と前記チェックコードとを関連付けて記憶するチェックコード記憶ステップと、
前記チェックコード記憶ステップにより記憶される前記

チェックコードのうち、前記読出ステップにより読み出された前記識別符号に対応する前記チェックコードと前記読出ステップにより読み出された前記チェックコードが一致するか否かを判別する判別ステップと、
前記判別ステップにより前記チェックコードが一致すると判別された場合、取引を許可し、前記チェックコードが一致しないと判別された場合、その電子マネーカードを不正カードと判別し、不正検出の旨を通知する制御ステップと、
取引が許可された場合、前記電子マネーカードに対して新たにチェックコードを生成するコード生成ステップと、
前記チェックコード記憶ステップにより記憶されている前記チェックコードのうち、該電子マネーカードのチェックコードを前記生成ステップにより生成された前記チェックコードに更新する更新ステップと、
前記電子マネーカードに記憶されている前記チェックコードを前記チェックコード記憶ステップにより記憶されている前記チェックコードと同一の値に更新するステップと、
を備える、ことを特徴とする不正カード検出方法。
【請求項１２】前記更新ステップは、更新前の前記チェックコードを記憶する使用済チェックコード記憶ステップを更に備え、
前記制御ステップは、前記判別ステップにより前記チェックコードが一致しないと判別された場合、前記電子マネーカードに記憶されている前記チェックコードが前記使用済チェックコード記憶ステップにより記憶されたチェックコードのいずれかと一致するか否かを判別し、一致した場合、不正に複製されたコピーカードの検出を通知する手段を更に備える、
ことを特徴とする請求項１１に記載の不正カード検出方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、金銭的情報である電子マネーを取引する電子マネーシステム及び不正カード検出方法に関する。
【０００２】
【従来の技術】貨幣的価値を有する金銭データを用いて電子的な決済を可能とする電子マネーシステムが例えば、特公平７－１１１７２３等に開示されている。電子マネーシステムでは、図１０に示すように、本物（オリジナル）の電子マネーカード（金銭データを記録したＩＣカード）と全く同一のデータを記憶したコピーカードを作成し、使用することが論理的に可能である。
【０００３】
【発明が解決しようとする課題】このため、電子マネーシステムでは、本物の電子マネーカードをコピーする等により作成された偽造カードの使用を防止する必要があ

る。また、カードの真正な所有者のみが、そのカードを使用できるようにすることが望ましい。しかし、このような要請を満たす電子マネーシステムは、未だに、提案されていない。

【０００４】本発明は、上記実状に鑑みてなされたもので、偽造されたカードの不正使用を有効に防止することができる電子マネーシステム及び不正カード検出方法を提供することを目的とする。

【０００５】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係る電子マネーシステムは、金銭的価値を有する電子マネーを格納する電子マネーカードと、該電子マネーカードを処理するための端末と、該端末を制御するセンタとを備え、前記電子マネーカード間で前記電子マネーを取引する電子マネーシステムであって、前記電子マネーカードは、該電子マネーカードを特定するための識別符号と、チェックコードとを記憶する手段を備え、前記端末は、前記電子マネーカードに記憶されている前記チェックコードと前記識別符号とを含む取引要求を前記センタに送信する送信手段を備え、前記センタは、各前記電子マネーカードの前記チェックコードを記憶するチェックコード記憶手段と、前記チェックコード記憶手段に記憶されている前記チェックコードのうち、前記端末からの前記取引要求に含まれている前記識別符号により特定される前記電子マネーカードの前記チェックコードが前記取引要求に含まれている前記チェックコードと一致するか否かを判別する判別手段と、前記チェックコードが一致すると判別された場合、取引を許可し、前記チェックコードが一致しないと判別された場合、取引を中止する制御手段と、取引が許可された場合、前記電子マネーカードに対して新たにチェックコードを生成する生成手段と、前記チェックコード記憶手段に記憶されている該電子マネーカードの前記チェックコードを前記生成手段により生成された前記チェックコードに更新する第１の更新手段と、前記端末に装着されている前記電子マネーカードに記憶されている前記チェックコードを前記チェックコード記憶手段に記憶されている前記チェックコードと同一の値に更新するよう指示する手段と、を備え、前記端末は、前記センタからの指示に応答して、装着されている前記電子マネーカードの前記チェックコードを更新する第２の更新手段を更に備える。

【０００６】このような構成によれば、電子マネーカードのチェックコードが、センタに登録されている同電子マネーカードのチェックコードと一致するか否かを判別することにより、偽造等による不正カードの使用を防止することができる。また、使用された電子マネーカードのチェックコードと、センタが記憶する同電子マネーカードのチェックコードを、１回の取引毎に同一の値に更新する。これにより、その電子マネーカードのコピーカードが作成されていたとしても、使用された電子マネーカード以外のカードのチェックコードは、センタに登録されているチェックコードと異なってしまうため、使用できなくなる。よって、コピーカードの不正使用を防止することができる。

【０００７】前記制御手段は、前記判別手段により前記チェックコードが一致しないと判別された場合、不正検出を通知する手段を更に備えてもよい。これにより、不正カードの使用を検出することができる。

【０００８】前記第１の更新手段は、更新前の前記チェックコードを記憶する使用済チェックコード記憶手段を更に備えてもよく、前記制御手段は、前記判別手段により前記チェックコードが一致しないと判別された場合、前記電子マネーカードに記憶されている前記チェックコードが前記使用済チェックコード記憶手段に記憶されている前記チェックコードのいずれかと一致するか否かを判別し、一致した場合、不正に複製されたコピーカードの検出を通知する手段を更に備えてもよい。これにより、コピーカードの不正使用を検出することができる。

【０００９】前記生成手段は、乱数を用いて新たなチェックコードを生成する手段を更に備えてもよい。これにより、生成されるチェックコードを予測することが困難となり、信頼性の高いマネーシステムを実現することができる。

【００１０】前記電子マネーカードは、光エネルギーが照射されることにより物理的にピットが形成されてデータが書き込まれ、書き換えが実質的に不可能な光記憶部を備え、該光記憶部に取引に関する情報を記録してもよい。これにより、データの改ざん、偽造がより困難となるため、システムの信頼性を高めることができる。

【００１１】この発明の第２の観点にかかる電子マネーシステムは、金銭的価値を有する電子マネーを格納する電子マネーカードを用いて前記電子マネーを取引する電子マネーシステムにおいて、前記電子マネーカードは、前記電子マネーカードを特定するための識別符号とチェックコードを記憶する記憶手段を備え、前記電子マネーカードに記憶されている前記チェックコードと前記識別符号とを読み出す読出手段と、各前記電子マネーカードの前記識別符号と前記チェックコードを関連付けて記憶するチェックコード記憶手段と、前記チェックコード記憶手段に記憶される前記チェックコードのうち、前記読出手段により読み出された前記識別符号に対応する前記チェックコードと、前記読出手段により読み出された前記チェックコードが一致するか否かを判別するコード判別手段と、前記コード判別手段により前記チェックコードが一致すると判別された場合、取引を許可し、前記チェックコードが一致しないと判別された場合、取引を中止する制御手段と、取引が許可された場合、前記電子マネーカードに対して新たにチェックコードを生成する生成手段と、前記チェックコード記憶手段に記憶されてい

る前記チェックコードのうち、該電子マネーカードの前記チェックコードを前記生成手段により生成された前記チェックコードに更新する手段と、前記電子マネーカードに記憶されている前記チェックコードを前記チェックコード記憶手段に新たに記憶される前記チェックコードと同一の値に更新する手段と、を備える。

【００１２】このような構成によれば、電子マネーカードのチェックコードが、チェックコード記憶手段に登録されている同電子マネーカードのチェックコードと一致するか否かを判別することにより、偽造等による不正カードの使用を防止することができる。また、使用された電子マネーカードのチェックコードと、チェックコード記憶手段が記憶する同電子マネーカードのチェックコードを、１回の取引毎に同一の値に更新する。これにより、その電子マネーカードのコピーカードが作成されていたとしても、チェックコードが異なってしまうため、使用不可となる。よって、コピーカードの不正使用を防止することができる。

【００１３】上記第１と第２の観点に係る電子マネーシステムにおいて、前記電子マネーカードに、該電子マネーカードの保有者の身体的特徴を記憶させてもよく、前記電子マネーカードの利用者の身体的特徴を読み取り、該電子マネーカードに記憶されている前記身体的特徴と比較し、類似度が一定値以上か否かを判別し、類似度が一定値以上である場合、前記取引要求の送信を許可してもよい。

【００１４】このような構成によれば、電子マネーカードが使用される際、利用者の身体的特徴を読み取り、その電子マネーカードに記憶されているカード保有者の身体的特徴と照合することにより、利用者がその電子マネーの保有者か否かを判別する。これにより、他者が電子マネーカードの保有者になりすまして、その電子マネーカードを使用することを防止することができる。

【００１５】前記身体的特徴は、例えば、指紋、声紋、顔の画像、網膜パターンに関する情報のいずれかを含む。

【００１６】この発明の第３の観点にかかる電子マネーシステムは、金銭的価値を有する電子マネーを格納する電子マネーカードを用いて前記電子マネーを取引する電子マネーシステムにおいて、前記電子マネーカードはチェックコードを記憶し、各前記電子マネーカードの前記チェックコードを記憶するチェックコード記憶手段と、取引に用いる前記電子マネーカードに記憶される前記チェックコードが、前記チェックコード記憶手段に記憶されている前記チェックコードのうちの前記取引に用いる電子マネーカードの前記チェックコードと一致するか否かを判別し、一致する場合取引を許可し、一致しない場合取引を中止すると共に不正検出を通知する判別手段と、取引が許可された場合、前記電子マネーカードに記憶されている前記チェックコードと前記チェックコード

記憶手段に記憶されている前記電子マネーカードの前記チェックコードとを同一の新たな値に更新する手段と、を備える。

【００１７】このような構成によれば、電子マネーカードのチェックコードが、登録されている同電子マネーカードのチェックコードと一致するか否かを判別することにより、偽造等による不正カードを防止することができる。また、使用された電子マネーカードが記憶するチェックコードと、チェックコード記憶手段が記憶する同電子マネーカードのチェックコードを、１回の取引毎に同一の値に更新する。これにより、その電子マネーカードのコピーカードが作成され、使用されたとしても、チェックコードが異なってしまうため、不正カードとして検出できる。

【００１８】この発明の第４の観点にかかる不正カード検出方法は、金銭的価値を有する電子マネーを格納する電子マネーカードを用いて電子マネーを取引する電子マネーシステムにおいて、各前記電子マネーカードを特定するための識別符号とチェックコードを該電子マネーカードに記憶させる記憶ステップと、前記電子マネーカードから前記チェックコードと前記識別符号とを読み出す読出ステップと、各前記電子マネーカードの前記識別符号と前記チェックコードとを関連付けて記憶するチェックコード記憶ステップと、前記チェックコード記憶ステップにより記憶される前記チェックコードのうち、前記読出ステップにより読み出された前記識別符号に対応する前記チェックコードと前記読出ステップにより読み出された前記チェックコードが一致するか否かを判別する判別ステップと、前記判別ステップにより前記チェックコードが一致すると判別された場合、取引を許可し、前記チェックコードが一致しないと判別された場合、その電子マネーカードを不正カードと判別し、不正検出の旨を通知する制御ステップと、取引が許可された場合、前記電子マネーカードに対して新たにチェックコードを生成するコード生成ステップと、前記チェックコード記憶ステップにより記憶されている前記チェックコードのうち、該電子マネーカードの前記チェックコードを前記生成ステップにより生成された前記チェックコードに更新する更新ステップと、前記電子マネーカードに記憶されている前記チェックコードを前記チェックコード記憶ステップにより記憶されている前記チェックコードと同一の値に更新するステップと、を備える。

【００１９】このような構成によれば、電子マネーカードのチェックコードが、チェックコード記憶ステップにより記憶されている同電子マネーカードのチェックコードと一致するか否かを判別することにより、偽造等による不正カードの使用を防止することができる。また、使用された電子マネーカードのチェックコードと、チェックコード記憶ステップにより記憶される同電子マネーカードのチェックコードを、１回の取引毎に同一の値に更

新する。これにより、その電子マネーカードのコピーカードが作成されていたとしても、チェックコードが異なってしまうため、使用不可となる。よって、コピーカードの不正使用を防止することができる。

【００２０】前記更新ステップは、更新前の前記チェックコードを記憶する使用済チェックコード記憶ステップを更に備え、前記制御ステップは、前記判別手段により前記チェックコードが一致しないと判別された場合、前記電子マネーカードに記憶されている前記チェックコードが前記使用済チェックコード記憶ステップにより記憶されたチェックコードのいずれかと一致するか否かを判別し、一致した場合、コピーカードの検出を通知する手段を更に備える。これにより、コピーカードの不正使用を検出することができる。

【００２１】

【発明の実施の形態】以下、この発明の実施の形態にかかる電子マネーシステムについて図面を参照して説明する。この電子マネーシステムは、図１に示すように、電子マネー管理センタ１１と、銀行センタ１２と、電子マネー端末１３と、電子マネーカード１５と、より構成される。

【００２２】電子マネー管理センタ１１は、この電子マネーシステム全体の動作を制御（管理）するコンピュータシステムである。電子マネー管理センタ１１は、このシステムにおいて使用可能な電子マネーカード１５の情報を格納するための利用者データベース（ＤＢ）１７を備える。利用者ＤＢ１７は、図２に示すように、電子マネーカード１５のカードＩＤ（識別符号）、電子マネーカード１５の正当性をチェックするためのチェックコード、残高、等を記憶する。

【００２３】また、電子マネー管理センタ１１は、利用者ＤＢ１７に記憶されている各電子マネーカード１５のデータに対して一時に１ユーザしかアクセスできないよう排他制御するＤＢ制御部１８を備える。ＤＢ制御部１８は、図３に示すような、利用者ＤＢ１７に記憶されている各電子マネーカード１５のデータに対するアクセス状況をチェックするためのアクセステーブルを有する。図示されるように、アクセステーブルは、各電子マネーカード１５のカードＩＤと、そのカードＩＤのデータがアクセス中か否か（”ＯＮ”か”ＯＦＦ”）を示すアクセスフラグの項目を備える。例えば、図３に示すアクセステーブルは、アクセスフラグが”ＯＮ”であるカードＩＤ”Ｃ０６”と”Ｃ１０”のデータがアクセス中であることを示す。

【００２４】ＤＢ制御部１８は、利用者ＤＢ１７のデータにアクセス要求が発生すると、アクセス要求対象のデータのアクセスフラグを参照し、アクセスフラグが”ＯＦＦ”、即ちアクセスされていない場合、アクセスを許可する。また、アクセスを許可した際、そのアクセスフラグを”ＯＮ”、即ち”アクセス中”に更新する。アクセスが終了すると、そのアクセスフラグを再度”ＯＦＦ”に更新する。なお、アクセスフラグを参照した際、アクセスフラグが”ＯＮ”の場合は、アクセスフラグが”ＯＦＦ”になるまで待つ。

【００２５】銀行センタ１２は、電子マネーカード１５の利用者（保有者）の口座である決済口座と、銀行が保有する電子マネーの運用口座である別段口座とを備え、これらの口座の入出金処理を行う。例えば、銀行センタ１２は、電子マネー管理センタ１１からの指示に従って、電子マネーカード１５の利用者の決済口座から別段口座への振り替え及び別段口座から決済口座への振り替えを行う。

【００２６】電子マネー端末１３は、利用者が電子マネーカード１５を挿入又は装着し、所定の操作をすることにより、電子マネーの取引をするための端末である。電子マネー端末１３は、図４に示すように、入力部３１と、表示部３２と、カード処理部３３と個人情報読取部３４を備える。

【００２７】入力部３１は、電子マネーの取引の指示等を入力する。表示部３２は、処理メニュー、メッセージ等を表示する。カード処理部３３は、電子マネーカード１５を受け付ける挿入口と、後述する電子マネーカード１５のＩＣ部２０をアクセスするためのＩＣリード／ライト部と、光記憶部２１をアクセスするための光記憶リード／ライト部とを備える。

【００２８】個人情報読取部３４は、利用者の身体的特徴による特有情報（指紋）を読みとるための装置である。個人情報読取部３４の構成の一例を図５に示す。個人情報読取部３４は、指紋をスキャンするための読取窓（図示せず）を備え、読取窓内の画像（指紋の画像）をスキャンし、画像データを取得する画像取得部５１と、画像取得部５１で取得した画像データをフーリエ変換するフーリエ変換部５２と、フーリエ変換部５２で取得されたフーリエ級数の位相情報のみを抽出する位相情報抽出部５３と、位相情報抽出部５３で生成された位相情報と後述する電子マネーカード１５のＩＣ部２０から読み出した位相情報とを合成する合成部５４と、合成部５４で合成された位相情報をフーリエ変換して相関強度を取得するフーリエ変換部５５と、フーリエ変換部５５で得られた相関強度と閾値を比較し、操作者が正当者であるか否かを判別する判別部５６を備える。

【００２９】また、電子マネー端末１３は、後述する支払い処理等で電子マネーカード１５から支払われた電子マネーを入金情報として記憶するための記憶部（図示せず）を備える。

【００３０】電子マネーカード１５は、例えば、図６に示すように、ＩＣ部（ＩＣチップ）２０と光記憶部２１を備える光ＩＣハイブリッドカードから構成される。ＩＣ部２０は制御回路とメモリ回路を内蔵する。このメモリ回路は、図６に示すように、動作プログラムの他に、

カードＩＤ、電子マネーの残高、チェックコード、等を記憶する。光記憶部２１は、例えば、光エネルギーが照射されることによりピット等が形成されてデータが書き込まれるタイプの書き換え不可能な追記型の記憶媒体等から構成され、この電子マネーカード１５の所有者の指紋データ、電子マネーの取引情報等を記憶する。この指紋データは、例えば、上述の画像取得部５１とフーリエ変換部５２と位相情報抽出部５３とを備える指紋読取機で取得した位相情報である。

【００３１】取引情報は、図７に示すように、取引区分（チャージ（残高の補充）、支払い、譲渡、換金等）、取引日時、取引金額、取引先カードＩＤ、取引のために電子マネーカードが装着された電子マネー端末１３の端末ＩＤ、等の項目により構成される。

【００３２】この電子マネーシステムでは、取引に先だって、利用者の指紋データを取得し、電子マネーカード１５に記憶されている指紋データと照合することにより、その利用者の正当性をチェックする。以下、この照合処理について説明する。まず、利用者が、例えば図８（Ａ）に示すような、電子マネー端末１３の表示部３２に表示された処理メニューの中から所望の処理を選択する。これに応答し、電子マネー端末１３は、図８（Ｂ）に示すような、電子マネーカード１５をカード処理部３３に挿入し、個人情報読取部３４上に指を置くよう指示する旨のメッセージを表示する。

【００３３】利用者がメッセージに従って個人情報読取部３４上に指を置くと、個人情報読取部３４の画像取得部５１は、読取窓内の指紋をスキャンし、その画像を取り込む。フーリエ変換部５２は、読み取られた画像をフーリエ変換し、位相情報抽出部５３が位相情報を取り込む。

【００３４】続いて、合成部５４は、電子マネーカード１５の光記憶部２１に記憶されている位相情報を読み出し、位相情報抽出部から抽出された位相情報と合成し、さらに、フーリエ変換部５５は合成データをフーリエ変換し、相関強度を求める。

【００３５】判定部５６は、相関強度が一定値以上の場合、予め光記憶部２１に記憶されている指紋と読み取った指紋とが類似し、利用者が電子マネーカード１５の正当な保有者であると判別し、選択された処理に対応する以後の処理を可能とするように制御する。相関強度が一定値未満の場合、予め光記憶部２１に記憶されている指紋と読み取った指紋が類似しないと判断し、指紋照合が一致しないため以後の操作できない旨のメッセージを表示部３２に表示し、電子マネーカード１５を排出する。

【００３６】これにより、利用者の身体的特徴に基づいて、電子マネーカード１５の利用者が正当な者か否かを判別し、利用者が正当であると判別したとき、電子マネーの取引を許可する。よって、電子マネーカード１５の所有者以外の者による電子マネーカード１５の不正使用を有効に防止できる。

【００３７】利用者の指紋照合が正常に完了すると、処理メニューから選択された取引の処理が実行される。この電子マネーシステムにおける基本的な処理には、電子マネーチャージ処理（電子マネーカード１５に記憶される残高の補充）、電子マネー支払処理、電子マネー譲渡処理、電子マネー換金処理、等がある。これらの処理について、以下説明する。

【００３８】まず、電子マネーチャージ処理を図９を参照して説明する。なお、この場合の電子マネー端末１３の端末ＩＤを”Ｔ１５０”とし、電子マネーカード１５のカードＩＤを”Ｃ９９”、チェックコードを”Ｂ６ＷＲ５Ｖ”とする。利用者により選択された処理が、「１）電子マネーのチャージ」の場合、電子マネー端末１３は、この選択に応答し、図８（Ｃ）に示す金額入力画面を表示する。利用者は、チャージ金額として、例えば「１万円」を入力する。

【００３９】電子マネー端末１３は、この入力に応答し、電子マネーカード１５のＩＣ部２０からカードＩＤ”Ｃ９９”とチェックコード”Ｂ６ＷＲ５Ｖ”を読み出し、入力された取引金額”１万円”と共に取引要求（この場合、チャージ要求）として電子マネー管理センタ１１へ送信する。

【００４０】電子マネー管理センタ１１は、受信したチャージ要求に応答し、利用者ＤＢ１７に記憶されているデータのうちのカードＩＤ”Ｃ９９”のデータに対するアクセス要求をＤＢ制御部１８に送信する。ＤＢ制御部１８は、受信したアクセス要求が示すカードＩＤ”Ｃ９９”のアクセスフラグを参照し、アクセスフラグが”ＯＦＦ”、即ち、アクセスされていない状態ならば、そのカードＩＤ”Ｃ９９”のデータに対するアクセスを許可する。アクセスフラグが”ＯＮ”、即ち、アクセス中の場合は、アクセスフラグが”ＯＦＦ”になるまで待つ。

【００４１】ＤＢ制御部１８により、カードＩＤ”Ｃ９９”のデータに対するアクセスが許可されると、電子マネー管理センタ１１は、利用者ＤＢ１７上のチェックコードが、受信した電子マネーカード１５上のチェックコード”Ｂ６ＷＲ５Ｖ”と一致するか否か判別する。チェックコードが一致する場合、電子マネー管理センタ１１は、電子マネーカード１５を正規のカードと判別し、利用者ＤＢ１７のカードＩＤ”Ｃ９９”の残高に、指示された取引金額”１万円”を加算すると共に、カードＩＤ”Ｃ９９”の決済口座から別段口座へ”１万円”だけ振り替えるよう銀行センタ１２に指示する。この指示に応答して、銀行センタ１２は、カードＩＤ”Ｃ９９”の決済口座から別段口座へ”１万円”だけ振り替える。チェックコードが一致しない場合、電子マネー管理センタ１１は不正検出の旨のメッセージを表示し、管理者に通知すると共に取引を中止する。

【００４２】次に電子マネー管理センタ１１は、この電

子マネーカード１５に対して新たなチェックコードを例えば乱数を発生させて生成し、利用者ＤＢ１７上のカードＩＤ”Ｃ９９”のチェックコードを更新する。更新完了後、電子マネー管理センタ１１はＤＢ制御部１８にアクセス終了を通知する。これに応じて、ＤＢ制御部１８は、カードＩＤ”Ｃ９９”のアクセスフラグを”ＯＦＦ”に戻す。また、電子マネー管理センタ１１は、新たなチェックコードを含む取引完了信号を電子マネー端末１３に送信する。なお、チェックコードの生成方法に関しては、乱数に限定されず任意の手法を用いてもよい。

【００４３】電子マネー端末１３は、電子マネー管理センタ１１からの取引完了信号に応答して、挿入されている電子マネーカード１５のＩＣ部２０に記憶されているチェックコード”Ｂ６ＷＲ５Ｖ”を、受信した新たなチェックコードに更新し、残高に”１万円”だけ加算（チャージ）する。また、電子マネー端末１３は、電子マネーカード１５の光記憶部２１に、取引区分”チャージ”、取引日時、取引金額”１万円”、端末ＩＤ”Ｔ１５０”を含む取引情報を追記する。このようにして、１回の取引（この場合、チャージ）毎に、電子マネー管理センタ１１の利用者ＤＢ１７上のチェックコードと電子マネーカード１５上のチェックコードを同時に更新する。これにより、カードＩＤ”Ｃ９９”の電子マネーカード１５の複製カードが存在していたとしても、それらの複製カードのチェックコードが利用者ＤＢ１７上のチェックコードと異なってしまうため、使用できなくなる。よって、それら偽造カードの不正使用を防止することができる。

【００４４】以下、他の取引処理についても簡単に説明する。電子マネー支払処理を、利用者がある店舗で商品を購入し、その代金を支払う場合を例に説明する。なお、この場合、利用者が商品を購入した店舗の電子マネー端末１３の端末ＩＤを”Ｔ１７０”とし、電子マネーカード１５のカードＩＤを”Ｃ５３”、チェックコードを”ＤＣＲ３４Ｈ”とする。

【００４５】電子マネー端末１３は、利用者による選択である「２）電子マネーの支払い」に応答し、図８（Ｃ）に示す金額入力画面を表示する。利用者は、支払い金額として、例えば「８千円」を入力する。

【００４６】電子マネー端末１３は、この入力に応答し、電子マネーカード１５のＩＣ部２０からカードＩＤ”Ｃ５３”とチェックコード”ＤＣＲ３４Ｈ”を読み出し、入力された取引金額”８千円”と共に支払要求として電子マネー管理センタ１１の送信する。

【００４７】電子マネー管理センタ１１は、受信した支払要求に応答し、利用者ＤＢ１７に記憶されているデータのうちのカードＩＤ”Ｃ５３”のデータに対するアクセス要求をＤＢ制御部１８に送信する。ＤＢ制御部１８は、受信したアクセス要求が示すカードＩＤ”Ｃ５３”のアクセスフラグを参照し、アクセスフラグが”ＯＦＦ”ならば、そのデータに対するアクセスを許可する。アクセスフラグが”ＯＮ”ならば、アクセスフラグが”ＯＦＦ”になるまで待つ。

【００４８】カードＩＤ”Ｃ５３”のデータに対するアクセスが許可されると、電子マネー管理センタ１１は、利用者ＤＢ１７上のチェックコードが、受信した電子マネーカード１５上のチェックコード”ＤＣＲ３４Ｈ”と一致するか否か判別する。チェックコードが一致する場合、電子マネー管理センタ１１は、電子マネーカード１５を正規のカードと判別し、利用者ＤＢ１７のカードＩＤ”Ｃ５３”の残高から、指示された取引金額”８千円”だけ差し引く。チェックコードが一致しない場合、電子マネー管理センタ１１は不正検出の旨のメッセージを表示し、管理者に通知すると共に取引を中止する。

【００４９】次に電子マネー管理センタ１１は、この電子マネーカード１５に対して新たなチェックコードを例えば乱数を発生させて生成し、利用者ＤＢ１７上のカードＩＤ”Ｃ５３”のチェックコードを更新する。更新完了後、電子マネー管理センタ１１はＤＢ制御部１８にアクセス終了を通知する。これに応じて、ＤＢ制御部１８は、カードＩＤ”Ｃ５３”のアクセスフラグを”ＯＦＦ”に戻す。また、電子マネー管理センタ１１は、新たなチェックコードを含む取引完了信号を電子マネー端末１３に送信する。

【００５０】電子マネー端末１３は、電子マネー管理センタ１１からの取引完了信号に応答して、挿入されている電子マネーカード１５のＩＣ部２０に記憶されているチェックコード”ＤＣＲ３４Ｈ”を、受信した新たなチェックコードに更新し、残高から”８千円”だけ差し引く。また、電子マネー端末１３は、電子マネーカード１５の光記憶部２１に、取引区分”支払い”、取引日時、取引金額”８千円”、端末ＩＤ”Ｔ１７０”を含む取引情報を追記する。電子マネーカード１５への書き込みが完了すると、電子マネー端末１３は、”８千円”を入金情報として記憶する。

【００５１】次に、電子マネー譲渡処理について説明する。なお、この場合、譲渡元の電子マネーカード１５Ａのカードを”Ｃ６４”、チェックコードを”３ＥＲ５Ｙ６”とし、譲渡先の電子マネーカード１５Ｂのカードを”Ｃ７７”とし、電子マネー端末１３の端末ＩＤを”Ｔ１７０”とする。

【００５２】電子マネー端末１３は、利用者による選択である「３）電子マネーの譲渡」に応答し、図８（Ｃ）に示す金額入力画面を表示する。利用者は、譲渡金額として、例えば「２万円」を入力する。

【００５３】電子マネー端末１３は、この入力に応答し、譲渡元の電子マネーカード１５ＡのＩＣ部２０からカードＩＤ”Ｃ６４”とチェックコード”３ＥＲ５Ｙ６”を読み出し、譲渡先の電子マネーカード１５ＢのＩＣ部２０からカードＩＤ”Ｃ７７”を読み出し、入力さ

れた取引金額”２万円”と共に譲渡要求として電子マネー管理センタ１１に送信する。

【００５４】電子マネー管理センタ１１は、受信した譲渡要求に応答し、利用者ＤＢ１７に記憶されているデータのうち、譲渡元と譲渡先の電子マネーカード１５Ａ、１５ＢのカードＩＤ”Ｃ６４”、”Ｃ７７”のデータに対するアクセス要求をＤＢ制御部１８に送信する。ＤＢ制御部１８は、受信したアクセス要求が示すカードＩＤ”Ｃ６４”と”Ｃ７７”のアクセスフラグを参照し、アクセスフラグが共に”ＯＦＦ”ならば、そのデータに対するアクセスを許可する。いずれかのアクセスフラグが”ＯＮ”ならば、そのアクセスフラグが”ＯＦＦ”になるまで待つ。

【００５５】カードＩＤ”Ｃ６４”、”Ｃ７７”のデータに対するアクセスが許可されると、電子マネー管理センタ１１は、利用者ＤＢ１７上のカードＩＤが”Ｃ６４”のチェックコードが、受信した電子マネーカード１５Ａ上のチェックコード”３ＥＲ５Ｙ６”と一致するか否か判別する。チェックコードが一致する場合、電子マネー管理センタ１１は、電子マネーカード１５Ａを正規のカードと判別し、利用者ＤＢ１７のカードＩＤ”Ｃ６４”の残高から、指示された取引金額”２万円”だけ差し引き、カードＩＤ”Ｃ７７”の残高に、取引金額”２万円”を加算する。チェックコードが一致しない場合、電子マネー管理センタ１１は不正検出の旨のメッセージを表示し、管理者に通知すると共に取引を中止する。

【００５６】次に電子マネー管理センタ１１は、この電子マネーカード１５Ａに対して新たなチェックコードを例えば乱数を発生させて生成し、利用者ＤＢ１７上のカードＩＤ”Ｃ６４”のチェックコードを更新する。更新完了後、電子マネー管理センタ１１はＤＢ制御部１８にアクセス終了を通知する。これに応じて、ＤＢ制御部１８は、カードＩＤ”Ｃ６４”と”Ｃ７７”のアクセスフラグを”ＯＦＦ”に戻す。また、電子マネー管理センタ１１は、電子マネーカード１５Ａの新たなチェックコードを含む取引完了信号を電子マネー端末１３に送信する。

【００５７】電子マネー端末１３は、受信した取引完了信号に応答して、譲渡元の電子マネーカード１５ＡのＩＣ部２０のチェックコード”３ＥＲ５Ｙ６”を、受信した新たなチェックコードに更新し、残高から”２万円”だけ差し引き、取引区分”譲渡”と取引日時と取引金額”２万円”と譲渡先カードＩＤ”Ｃ７７”と端末ＩＤ”Ｔ１７０”を含む取引情報を追記する。また、電子マネー端末１３は、譲渡先の電子マネーカード１５ＢのＩＣ部２０の残高に”２万円”を加算し、電子マネーカード１５の光記憶部２１に、取引区分”譲渡”と取引日時と取引金額”２万円”と譲渡元ＩＤ”Ｃ６４”と端末ＩＤ”Ｔ１７０”を含む取引情報を追記する。

【００５８】次に、電子マネー換金処理について説明する。なお、この場合、電子マネーカード１５のカードＩＤを”Ｃ１４”、チェックコードを”ＭＮ５４Ｃ３”とし、電子マネー端末１３の端末ＩＤを”Ｔ２１０”とする。

【００５９】電子マネー端末１３は、利用者による選択である「４）電子マネーの換金」に応答し、図８（Ｃ）に示す金額入力画面を表示する。利用者は、換金金額として、例えば「３万円」を入力する。

【００６０】電子マネー端末１３は、この入力に応答し、電子マネーカード１５のＩＣ部２０からカードＩＤ”Ｃ１４”とチェックコード”ＭＮ５４Ｃ３”を読み出し、入力された取引金額”３万円”と共に換金要求として電子マネー管理センタ１１の送信する。

【００６１】電子マネー管理センタ１１は、受信した換金要求に応答し、利用者ＤＢ１７に記憶されているデータのうちのカードＩＤ”Ｃ１４”のデータに対するアクセス要求をＤＢ制御部１８に送信する。ＤＢ制御部１８は、受信したアクセス要求が示すカードＩＤ”Ｃ１４”のアクセスフラグを参照し、アクセスフラグが共に”ＯＦＦ”ならば、そのデータに対するアクセスを許可する。アクセスフラグが”ＯＮ”ならば、アクセスフラグが”ＯＦＦ”になるまで待つ。

【００６２】カードＩＤ”Ｃ１４”のデータに対するアクセスが許可されると、電子マネー管理センタ１１は、利用者ＤＢ１７上のカードＩＤ”Ｃ１４”のチェックコードが、受信した電子マネーカード１５上のチェックコード”ＭＮ５４Ｃ３”と一致するか否か判別する。チェックコードが一致する場合、電子マネー管理センタ１１は、電子マネーカード１５を正規のカードと判別し、利用者ＤＢ１７のカードＩＤ”Ｃ１４”の残高に、指示された取引金額”３万円”だけ差し引くと共に、別段口座からカードＩＤ”Ｃ１４”の決済口座へ”３万円”だけ振り替えるよう銀行センタ１２に指示する。この指示に応答して、銀行センタ１２は、別段口座からカードＩＤ”Ｃ１４”の決済口座へ”３万円”だけ振り替える。チェックコードが一致しない場合、電子マネー管理センタ１１は不正検出の旨のメッセージを表示し、管理者に通知すると共に取引を中止する。

【００６３】次に電子マネー管理センタ１１は、この電子マネーカード１５に対して新たなチェックコードを例えば乱数を発生させて生成し、利用者ＤＢ１７上のカードＩＤ”Ｃ１４”のチェックコードを更新する。更新完了後、電子マネー管理センタ１１はＤＢ制御部１８にアクセス終了を通知する。これに応じて、ＤＢ制御部１８は、カードＩＤ”Ｃ１４”のアクセスフラグを”ＯＦＦ”に戻す。また、電子マネー管理センタ１１は、新たなチェックコードを含む取引完了信号を電子マネー端末１３に送信する。

【００６４】電子マネー端末１３は、受信した取引完了信号に応答して、電子マネーカード１５のＩＣ部２０の

チェックコード”ＭＮ５４Ｃ３”を、受信した新たなチェックコードに更新し、残高から”３万円”だけ差し引き、取引区分”換金”と取引日時と取引金額”３万円”と端末ＩＤ”Ｔ１７０”を含む取引情報を追記する。

【００６５】以上説明したように、この電子マネーシステムでは、チャージ、支払い、譲渡、換金等の電子マネーの取引をした際に、取引に使用した電子マネーカード１５のチェックコードと利用者ＤＢ１７に登録されているチェックコードを同時に更新する。これにより、コピー等により偽造された不正カードのチェックコードが、利用者ＤＢ１７に登録されている新たなチェックコードと異なるコードとなるため、取引時にチェックコードを調べることにより、それらの不正カードの使用を防止することができる。

【００６６】なお、上記説明では、利用者から取得した指紋データと電子マネーカード１５に記憶されている指紋データとの照合をオフラインで処理しているが、これをオンラインで処理するようにしてもよい。この場合、電子マネー端末１３は、利用者から取得した指紋データと電子マネーカード１５上の指紋データを電子マネー管理センタ１１に送信する。電子マネー管理センタ１１は、受信した指紋データを照合し、その照合結果を電子マネー端末１３に送信する。また、電子マネー管理センタ１１に、このシステムの利用者の指紋データを記憶させておき、電子マネー端末１３が利用者から取得した指紋データのみを電子マネー管理センタ１１に送信し、電子マネー管理センタ１１が受信した指紋データと自己が記憶している指紋データを照合するようにしてもよい。

【００６７】また、電子マネー管理センタ１１がチェックコードを更新した際、更新前の古いチェックコードを不正コードリストとしてカードＩＤ毎に記憶してもよい。この場合、電子マネー管理センタ１１は、電子マネー端末１３から取引の要求を受信したとき、取引要求に含まれるチェックコードが、そのカードＩＤの不正コードリストのいずれかと一致するか否かを判別し、一致する場合は、コピーカード検出の旨のメッセージを表示し、取引を中止する。

【００６８】また、上記説明では、チェックコードの更新処理及び電子マネーの取引処理をオンラインで処理しているが、電子マネー端末１３が定期的に電子マネー管理センタ１１から利用者ＤＢ１７のデータをダウンロードすることにより、オフラインでチェックコードの更新処理及び電子マネーの取引処理を行うようにしてもよい。この場合、電子マネー端末１３は、取引完了後、更新後のチェックコード、取引の情報等を電子マネー管理センタ１１に送信する。電子マネー管理センタ１１は、受信した情報をもとに利用者ＤＢ１７を更新する。

【００６９】なお、指紋の類似度を判別する手法及び回路は図５に示す回路及び方法に限定されず、他の手法を使用してもよい。

【００７０】また、上記実施の形態においては、指紋の画像をフーリエ変換し、位相情報を抽出したものを指紋データとしてＩＣ部２０に格納したが、指紋を他の形式で変換して指紋データとしてもよい。例えば、指紋の画像の特定の位置のオン・オフを指紋データとしてもよい。

【００７１】また、指紋データに限定されず、声紋、顔のパターン、網膜パターン等の個人の身体的特徴を表す個人特定情報を指紋データの代わりに或いは指紋データと組み合わせて使用してもよい。例えば、個人情報読取部３４としてマイクロフォンを配置し、マイクロフォンで取得した音声の特徴データを抽出し、ＩＣ部２０に格納しておいた音声の特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別し、システムの使用を許可してもよい。

【００７２】また、顔のパターン、網膜パターン等を使用する場合には、顔、網膜パターンの特徴データをＩＣ部２０に格納し、カメラで取得した画像の特徴データを抽出し、ＩＣ部２０に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別するようにしてもよい。

【００７３】上記説明では、利用者の正当性を確認するために身体的特徴を用いたが、利用者にパスワード等を入力させて、その正当性を確認するようにしてもよい。

【００７４】なお、予め電子マネーカード１５に記憶させる特徴データは、ＩＣ部２０に格納してもよく、光記録部２１に格納してもよい。

【００７５】なお、電子マネーカード１５は、ＩＣ部（ＩＣチップ）２０と光記憶部２１を備えていればよく、その形状はカード型に限定されず任意である。

【００７６】また、ＤＢ制御部１８による排他制御の方法は、上述した方法に限定されず任意である。

【００７７】なお、この発明の電子マネー端末１３及び電子マネー管理センタ１１は、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行する電子マネー端末１３及び電子マネー管理センタ１１を構成することができる。

【００７８】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的に流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【００７９】

19

【発明の効果】以上説明したように、本発明によれば、使用された電子マネーカードが記憶するチェックコードと、センタが記憶する同電子マネーカードのチェックコードを、１回の取引毎に、同一のチェックコードに更新する。これにより、その電子マネーのコピーカードが作成されていたとしても、チェックコードが異なってしまうため、使用不可となる。よって、コピー等による偽造カードの不正使用を防止することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図２】利用者ＤＢの構造を示す図である。

【図３】アクセステーブルの構造を示す図である。

【図４】電子マネー端末の構成を示す図である。

【図５】個人情報読取部の構成の一例を示す図である。

【図６】電子マネーカードの構造を示す図である。

【図７】取引情報の構成を示す図である。

【図８】電子マネー端末の表示例を示す図である。

20

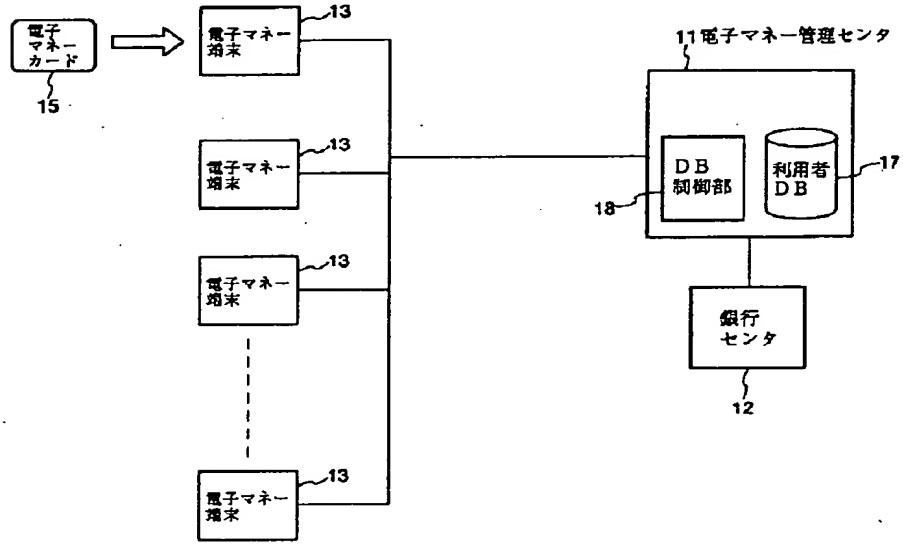
【図９】電子マネーチャージ処理を説明するための図である。

【図１０】電子マネーカードのコピーカードが使用可能な電子マネーシステムを説明するための図である。

【符号の説明】

１１　電子マネー管理センタ
１２　銀行センタ
１３　電子マネー端末
１５　電子マネーカード
１７　利用者ＤＢ
１８　ＤＢ制御部
２０　ＩＣ部
２１　光記憶部
３１　入力部
３２　表示部
３３　カード処理部
３４　個人情報読取部

【図１】

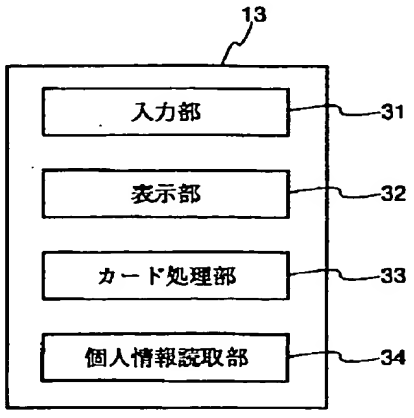


【図３】

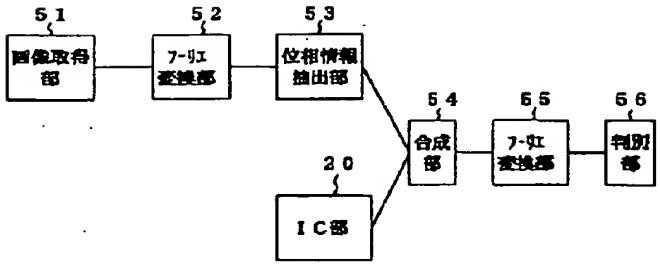
アクセステーブル

カードＩＤ	アクセスフラグ
Ｃ０１	ＯＦＦ
Ｃ０５	ＯＦＦ
Ｃ０６	ＯＮ
Ｃ０７	ＯＦＦ
Ｃ１０	ＯＮ
・	・
・	・
・	・
・	・
・	・

【図４】



【図５】

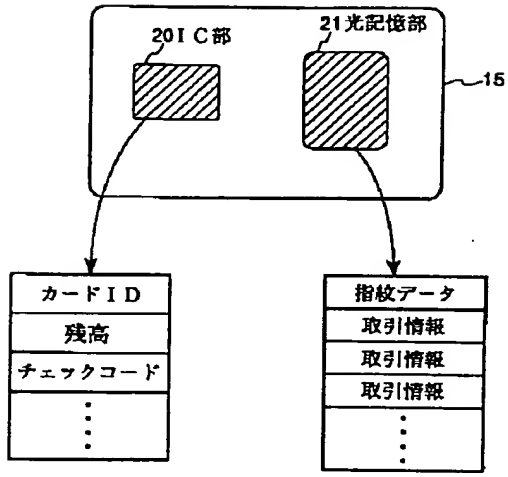


【図２】

利用者ＤＢ

カードＩＤ	チェックコード	残高
C01	ABF87G	20000
C05	2G41QS	55000
C06	Z9U62J	38000
C07	38HI0A	170000
C10	W3LGRP	86000
C15	349TJT	100000
・	・	・
・	・	・
・	・	・
・	・	・
・	・	・

【図６】

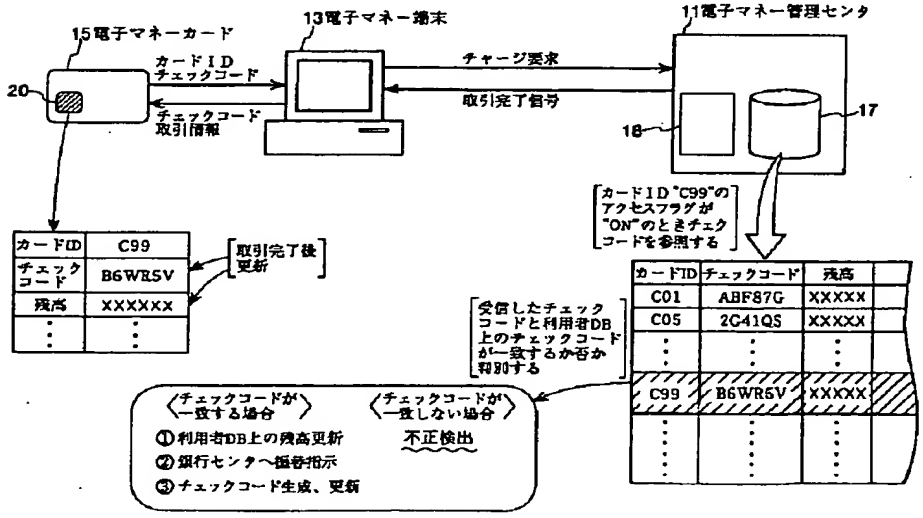


【図７】

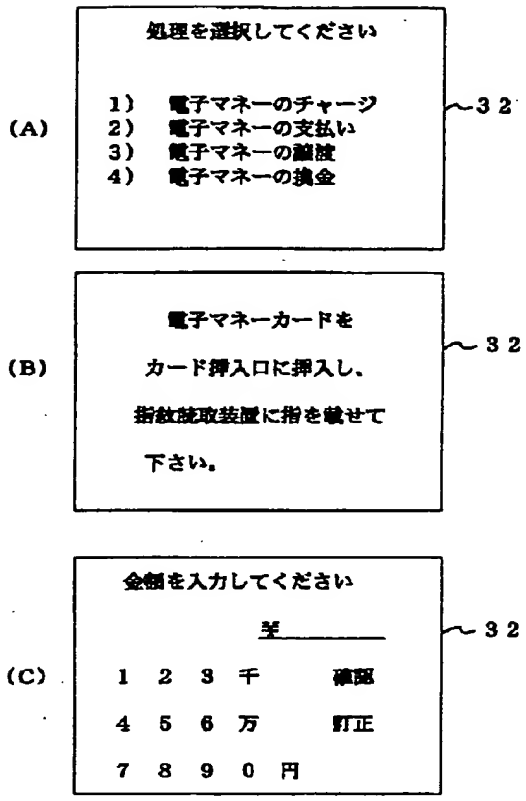
取引情報

取引区分	取引日時	取引金額	取引先カードＩＤ	端末ＩＤ
チャージ	H8／10／20	50000	*******	T122
支払い	H8／10／23	12000	*******	T131
チャージ	H8／10／26	20000	*******	T265
譲渡	H8／10／30	30000	C79	T148
換金	H8／11／7	10000	*******	T122
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

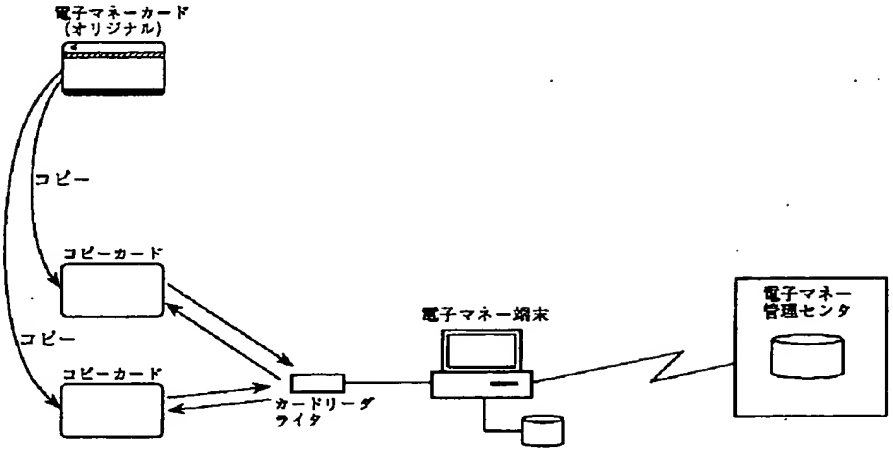
【図９】



【図８】



【図１０】



フロントページの続き

(51) Int. Cl.[6]	識別記号	FI		
Ｇ０７Ｆ　7/08		Ｇ０６Ｆ　15/30	３４０	
		Ｇ０７Ｆ　7/08		Ｚ

PARTIAL TRANSLATION OF JP 63(1988)-282579 A

Publication Date: November 18, 1988
Title of the Invention: INDIVIDUAL IDENTIFYING DEVICE
Patent Application Number: 62-115818
Filing Date: May 14, 1987
Inventors: Kazuyuki TSUNEYOSHI et al.
Applicant: TOSHIBA CORP.

(Page 4, left column, lines 4 – 19)
As described above, a retina pattern obtained when a light emitting device 30 illuminates, retina pattern information before the light emitting device 30 illuminates (i.e., retina pattern information written on an ID card), a retina pattern used when the retina pattern of a user of the ID card is compared, and a retina pattern obtained when the light emitting device 30 illuminates are compared with each other, whereby the reaction of the pupil is decided based on the presence/absence of a change. The decision information on the pupil reaction is sent to a main control part 21. The digital values of the retina pattern stored on the memory in the main control part 21 and the retina pattern information obtained from the ID card 6 are compared, bit by bit, to check whether or not the retina pattern matches with the retina pattern information. Further, it is judged from the decision information obtained from a pupil reaction decision part 34 whether or not the retina pattern is obtained from a living body. Consequently, it can be confirmed whether or not the ID card 6 corresponds to its owner.